

# MIROIR CIRCULAIRE ET POLYNÔMES DE STEWART

JEAN-CLAUDE CARREGA ET LABIB HADDAD

Comment peuvent se conjuguer deux variations sur un même thème, celui des constructions géométriques à l'aide de la règle et du compas, tel est le sujet de cette petite note.

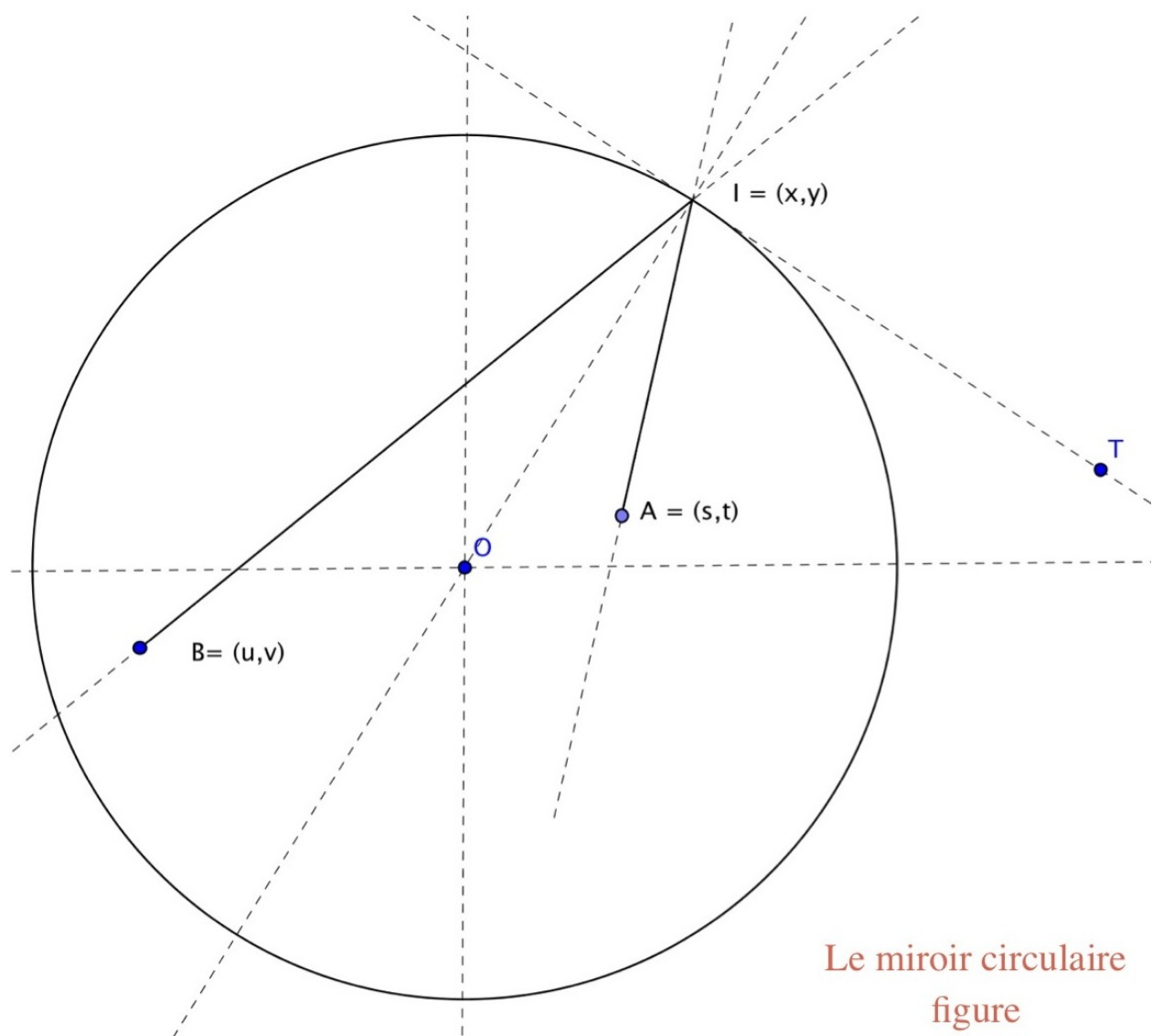
**Le polynôme de Stewart.** *Tout nombre constructible est algébrique sur le corps  $\mathbb{Q}$  et son degré est une puissance de 2. On le sait. On sait également que la réciproque est fausse : il y a des nombres non constructibles qui sont algébriques sur  $\mathbb{Q}$  et dont le degré est une puissance de 2. Le premier auteur de cette note en a donné les démonstrations dans un ouvrage destiné aux étudiants et aux enseignants du secondaire, *Théorie des corps, La règle et le compas* [1].*

Il a présenté, en particulier, le polynôme

$$X^4 - X - 1$$

comme contre-exemple à la réciproque. Il établit que ce polynôme est irréductible sur  $\mathbb{Q}$  et que l'une de ses deux racines réelles n'est pas constructible à l'aide de la règle et du compas bien qu'elle soit algébrique de degré  $4 = 2^2$ . Il attribue ce contre-exemple à IAN STEWART. En fait, le groupe de Galois de ce polynôme est le groupe symétrique  $S_4$  (comme on le voit, d'un clic, à l'aide du logiciel Maple) et, bien entendu, aucune de ses deux racines réelles n'est constructible.

En effet, dans le langage d'aujourd'hui, on énonce comme suit la caractérisation des nombres constructibles : un nombre  $\alpha$  est constructible, si et seulement si l'ordre de son groupe de Galois associé,  $\mathbf{G}(\alpha)$ , est une puissance de 2, ce qui n'est pas le cas du groupe symétrique  $S_4$ . Le résultat est détaillé dans le livre [1] déjà cité. On le trouve bien entendu, également, dans le van der Waerden [4]. On sait aussi que l'ordre du groupe de Galois  $\mathbf{G}(\alpha)$  est le degré  $[K : \mathbb{Q}]$  de l'extension  $K$  de  $\mathbb{Q}$ , où  $K$  est le corps de décomposition du polynôme minimal de  $\alpha$ . Voir [1], par exemple.



**Le miroir circulaire.** Dans le plan, on se donne une circonférence,  $C$ , et deux points,  $A$  et  $B$ . On cherche à construire les points  $I$  de  $C$  en lesquels le rayon lumineux  $AI$  se réfléchit pour repasser par  $B$ . Voir la figure ci-dessus.

C'est ce que l'on appelle le problème du miroir circulaire. On sait que cette construction est impossible à l'aide de la règle et du compas, sauf dans des cas très particuliers, pour certaines positions *critiques* des points  $A$  et  $B$ .

On a, parfois, appelé *problème d'Alhazen* ce problème du miroir circulaire (ou sphérique), voir [3]. On l'appelle aussi *problème du billard circulaire* (voir CARREGA [1, page 253, exercice 25]).

Voici le récit d'un lien que l'on tisse entre le miroir circulaire et le polynôme de Stewart.

## LES POLYNÔMES DE STEWART

Plus généralement, appelons *polynôme de Stewart* tout polynôme de la forme

$$S(X) = X^4 - rX - 1 \quad \text{où } r \text{ est un nombre rationnel non nul,}$$

ainsi que tous leurs multiples scalaires  $\lambda S(X)$  où  $\lambda$  est un nombre rationnel non nul.

Quitte à changer  $X$  en  $-X$ , on peut se ramener aux cas où l'on a  $r > 0$ .

En imitant ce qui est fait dans CARREGA [1, page 39], partant du polynôme

$$S(X) = X^4 - rX - 1,$$

on pose

$$r = a\sqrt{a^4 + 4}, \quad 2b = a^2 + \sqrt{a^4 + 4}, \quad 2\bar{b} = a^2 - \sqrt{a^4 + 4}.$$

Il vient :

$$S(X) = (X^2 + aX + b)(X^2 - aX + \bar{b}), \quad a^6 + 4a^2 - r^2 = 0.$$

Ainsi,  $a^2$  est racine du polynôme  $R(Y) = Y^3 + 4Y - r^2$  de degré 3. Ce polynôme est fonction strictement croissante de  $Y$  ; il prend des valeurs négatives pour  $Y < 0$  et possède donc une seule racine réelle laquelle est  $> 0$ . À cette racine réelle,  $a^2$ , correspondent deux valeurs opposées

$\pm a$ . On doit prendre, bien évidemment, la valeur qui a le même signe que  $r$ . On notera ainsi que  $a, b$  et  $\bar{b}$  sont des nombres réels, algébriques. Le discriminant du polynôme  $X^2 + aX + b$  est égal à  $a^2 - 4b$ , i.e.,  $-2\sqrt{a^4 + 4} - a^2 < 0$ ; celui du polynôme *conjugué*  $X^2 - aX + \bar{b}$  est égal à  $2\sqrt{a^4 + 4} - a^2 > 0$ .

Le polynôme de Stewart  $S(X)$  a toujours, ainsi, 4 racines distinctes, soit deux racines complexes conjuguées et deux racines réelles, à savoir

$$\frac{-a \pm i\sqrt{2\sqrt{a^4 + 4} + a^2}}{2}, \quad \frac{a \pm \sqrt{2\sqrt{a^4 + 4} - a^2}}{2}.$$

**Irréductibilité.** Soit  $\mathbb{A}$  le corps des nombres algébriques réels. Le polynôme de Stewart  $S(X)$  est ainsi décomposable dans  $\mathbb{A}[X]$  en un produit de deux polynômes de degré 2 : le polynôme  $U(X) = X^2 + aX + b$  et le polynôme  $V(X) = X^2 - aX + \bar{b}$ . Pour qu'il soit décomposable dans  $\mathbb{Q}[X]$ , il faut et il suffit que l'une des deux conditions suivantes soit remplie :

- (C1) Il existe un nombre rationnel  $s$  non nul tel que l'on ait  $r = s^3 - 1/s$ .
- (C2) Il existe un nombre rationnel  $a$  tel que l'on ait  $r^2 = a^6 + 4a^2$ .

**En effet**, la condition C1 revient à dire que le polynôme  $S(X)$  possède une racine rationnelle ce qui équivaut à dire qu'il se décompose dans  $\mathbb{Q}[X]$  en un produit d'un polynôme de degré 1 avec un polynôme de degré 3. Quant à la condition C2, elle implique que  $\sqrt{a^4 + 4} = r/a$  est un nombre rationnel. Cela entraîne que les coefficients  $a, b$  et  $\bar{b}$  sont rationnels, de sorte que les polynômes  $U(X)$  et  $V(X)$  appartiennent à  $\mathbb{Q}[X]$  : le polynôme  $S(X)$  se décomposerait alors dans  $\mathbb{Q}[X]$  en un produit de deux polynômes du second degré. Réciproquement, si  $S(X)$  était produit de deux polynômes de  $\mathbb{Q}[X]$ , du second degré, ces deux polynômes seraient  $U(X)$  et  $V(X)$ , *par nécessité*, d'où le résultat. **cqfd**

**Nota.** On signale toutefois ceci. La condition C2 n'est jamais satisfaite : on en donnera la démonstration dans l'APPENDICE ci-dessous. Cela veut dire qu'un polynôme de Stewart ne se décompose jamais en un produit de deux polynômes du second degré dans  $\mathbb{Q}[X]$ . Autrement dit,  $S(X)$  est réductible sur  $\mathbb{Q}$  si et seulement s'il possède une racine rationnelle.

Dans tous les autres cas, le polynôme  $S(X)$  est irréductible sur  $\mathbb{Q}$ , en particulier pour  $r = 1$ , le cas *princeps*.

**Le cas où  $r$  est entier.** Plus généralement, lorsque  $r$  est un entier (non nul), le polynôme  $S(X)$  est irréductible. Pour le voir, on montre que la condition C1 n'est pas satisfaite. Si l'on avait  $r = s^3 - 1/s$  où  $s = p/q$  est une fraction irréductible, on aurait  $p^4 - rpq^3 - q^4 = 0$ , donc  $p$  diviserait  $q$  et  $q$  diviserait  $p$ , de sorte que  $s = p/q$  serait égale à  $\pm 1$  et  $r$  serait nul, ce qui n'est pas !

Lorsque  $r$  est entier, si  $a^2$  est rationnel, c'est un entier. En effet,  $a^2$  est racine réelle positive du polynôme  $R(Y)$ . Si  $a^2$  est rationnelle, on l'écrit sous forme irréductible  $a^2 = p/q$ . Il vient  $p^3 + 4pq^2 - r^2q^3 = 0$ , donc  $q$  divise  $p$  et  $a^2$  est un entier.

Lorsque  $r$  est entier, on peut montrer simplement, directement, que la condition C2 n'est pas satisfaite, comme suit. Si l'on avait  $r = a\sqrt{a^4 + 4}$  pour  $a$  rationnel,  $a^2$  serait entier, d'après ce qui précède. On aurait  $a^4 + 4 = (r/a)^2$ , de sorte que  $u = r/a$  serait entier et l'on aurait

$$4 = u^2 - a^4 = (u - a^2)(u + a^2), \quad 0 < u - a^2 < u + a^2.$$

La seule possibilité serait alors  $u - a^2 = 1$  et  $u + a^2 = 4$  ce qui entraîne  $2u = 5$ , impossible puisque  $u$  est entier.

**Le cas où  $r$  est un nombre premier.** On suppose que  $r$  est un nombre **premier**. On établit que le polynôme  $R(Y)$  est irréductible. Pour cela, on doit montrer que sa racine  $t = a^2$  n'est pas rationnelle. D'après ce qui précède, il suffit de montrer que  $t$  n'est pas un entier !

**Démonstration.** On a  $t(t^2 + 4) = r^2$ . Si  $t$  était entier, il diviserait  $r^2$ . Or,  $r$  étant premier, on ne peut avoir que  $t = 1$  ou  $t = r$  ou  $t = r^2$ .  
 Si  $t = 1$ , on aurait  $r^2 = 5$  qui est impossible.  
 Si  $t = r$ , on aurait  $r^2 - r + 4 = 0$  qui n'a pas de racine réelle.  
 Si  $t = r^2$ , on aurait  $r^4 + 4 = 1$  qui est impossible. □

Ainsi  $t = a^2$  n'est pas un nombre constructible et il en résulte que  $a$  non plus n'est pas constructible. Les deux racines réelles du second facteur  $X^2 - aX + \bar{b}$  de  $S(X)$  ont pour somme  $a$ , donc l'une au moins de ses racines n'est pas constructible. Ainsi, l'ordre du groupe de Galois de  $S(X)$  n'est pas une puissance de deux.

En fait, aucune des 2 racines réelles de ce polynôme n'est constructible car toutes deux ont le même polynôme minimal  $S(X)$  [et l'ordre du groupe de Galois de  $S(X)$  n'est pas une puissance de deux].

Ainsi, les polynômes de Stewart  $S(X)$  avec  $r$  nombre premier permettent d'obtenir, par leurs racines réelles, une infinité de nombres algébriques de degré 4 qui ne sont pas constructibles.

**Une variante.** À la fin de la démonstration précédente, on peut tout aussi bien utiliser l'exercice 24 de [1], pages 252-253. Dans le a) de cet exercice, on fait démontrer le résultat général suivant au sujet des polynômes de degré 4 : *une racine réelle d'un polynôme irréductible  $P(X) \in \mathbb{Q}[X]$  de degré 4 est constructible si et seulement si le résolvant de  $P(X)$  est réductible sur  $\mathbb{Q}$ .* En l'occurrence, le résolvant du polynôme de Stewart  $S(X)$  n'est autre que le polynôme  $Y^3 + 4Y + r^2 = -R(-Y)$ , ce qui achève la démonstration.

**Remarque.** Examinons l'exemple où  $r = 4$ , un entier non premier. Dans ce cas, 2 est racine de  $R(Y) = Y^3 + 4Y - 16$ , de sorte que l'on a  $t = a^2 = 2$  et  $a = \sqrt{2}$ . Les 2 racines réelles de  $S(X)$ , données par les formules ci-dessus (en haut de la page 4) avec  $a = \sqrt{2}$ , sont constructibles et algébriques et de degré 4.

## LE MIROIR CIRCULAIRE

Dans le plan, on se donne une circonférence,  $C$ , et deux points,  $A$  et  $B$ . On cherche les points  $I$  de  $C$  en lesquels le rayon lumineux  $AI$  se réfléchit pour repasser par  $B$ .

Voici une solution analytique, à suivre sur la figure en page 2, ci-dessus.

Dans le plan des  $x, y$ , ayant  $O$  pour origine, on prend la circonférence

$$(C) \quad x^2 + y^2 = 1$$

ainsi que les points  $A = (s, t)$  et  $B = (u, v)$ . Soit  $IT$  la tangente en  $I$  à  $C$ . On voudrait trouver les points  $I = (x, y)$  de  $C$  tels que les droites  $IO$  et  $IT$  soient les deux bissectrices des angles que forment les droites  $IA$  et  $IB$ .

Il faut et il suffit pour cela que le rapport anharmonique des pentes des droites  $IA, IB, IO, IT$ , soit égal à  $-1$ . On a

$$p_{IA} = \frac{y-t}{x-s}, \quad p_{IB} = \frac{y-v}{x-u}, \quad p_{IO} = \frac{y}{x}, \quad p_{IT} = -\frac{x}{y}.$$

Ainsi, il faut et il suffit que l'on ait :

$$\frac{\frac{y-t}{x-s} - \frac{y}{x}}{\frac{y-v}{x-u} - \frac{y}{x}} : \frac{\frac{y-t}{x-s} + \frac{x}{y}}{\frac{y-v}{x-u} + \frac{x}{y}} = -1.$$

Tous calculs faits, cela donne :

$$(tx - sy)(x^2 + y^2 - ux - vy) + (vx - uy)(x^2 + y^2 - sx - ty) = 0.$$

Puisque  $x^2 + y^2 = 1$ , on obtient

$$(H) \quad (sv + tu)(y^2 - x^2) + 2(su - tv)xy + (t + v)x - (s + u)y = 0,$$

l'équation d'une hyperbole, H, passant par l'origine O.

En utilisant la paramétrisation classique suivante du cercle

$$x = \frac{1 - z^2}{1 + z^2}, \quad y = \frac{2z}{1 + z^2},$$

et tous calculs faits, l'équation  $H$  prend la forme que voici :

$$\frac{Q(z)}{(1 + z^2)^2} = 0,$$

où  $Q(z)$  est le polynôme suivant de degré 4 en  $z$  :

$$\begin{aligned} Q(z) = & (sv + tu + t + v)z^4 + 2(2su - 2tv + s + u)z^3 \\ & - 6(sv + tu)z^2 - 2(2su - 2tv - s - u)z + (sv + tu - t - v). \end{aligned}$$

Par commodité, on dira que ces polynômes  $Q(z)$  ainsi que tous leurs multiples scalaires  $\lambda Q(z)$  sont les *polynômes d'Alhazen*.

On montre alors que tout polynôme de Stewart est un polynôme d'Alhazen.

Pour cela, on spécialise une première fois, en prenant

$$t = s \text{ et } v = -u.$$

Le polynôme  $Q(z)$  prend la forme

$$Q(z) = (s - u)z^4 + 2(4su + s + u)z^3 - 2(4su - s - u)z - (s - u).$$

On spécialise de nouveau, en prenant

$$u = \frac{-s}{4s + 1}.$$

Le polynôme  $Q(z)$  s'écrit :

$$Q(z) = \frac{2s(2s + 1)}{4s + 1}(z^4 - rz - 1) \text{ où } r = \frac{-8s}{2s + 1}.$$

Il en découle, comme annoncé, que **tout polynôme de Stewart est un polynôme d'Alhazen.**

Le polynôme de Stewart  $S(X) = X^4 - rX - 1$  dépend du seul paramètre  $r$ . Le polynôme d'Alhazen  $Q(z)$  dépend des 4 paramètres  $s, t, u, v$ , les coordonnées des points  $A$  et  $B$ .

Dans CARREGA [1, p. 266, solution de l'exercice 25 sur le billard circulaire] on trouve l'expression suivante du polynôme  $Q(z)$

$$(a + 1)cz^4 + 2(a + b + 2ab)z^3 - 6acz^2 + 2(a + b - 2ab)z + (a - 1)c,$$

obtenue en utilisant les nombres complexes pour exprimer l'égalité des deux arguments correspondant aux angles définis par la bissectrice, cela étant fait dans le cas particulier où  $s = a, t = 0, u = b, v = c$ .

\* \* \*

Cette étude a permis la rencontre improbable des noms de deux mathématiciens que 10 siècles séparent : Ian Stewart est professeur émérite à l'université de Warwick en Angleterre. Il est l'auteur de nombreux ouvrages remarquables. Ibn Al Haytham (965 - 1039), connu en Occident sous le nom de Alhazen, est un savant du monde médiéval arabo-musulman, originaire de Perse. Il est l'auteur de traités sur la Géométrie, l'Optique et l'Astronomie.

\* \* \*

Pour les groupes de Galois des équations de degré 3 et 4, on pourra consulter utilement le livre de Kaplansky, [2].



## APPENDICE

EULER a montré ceci : *La somme de deux bicarrés d'entiers non nuls n'est jamais le carré d'un entier non nul.* Autrement dit, l'équation  $x^4 + y^4 = z^2$  n'a pas de solutions en entiers  $x, y, z$ , strictement positifs.

{Voir à ce sujet le livre de L. E. DICKSON, *Theory of numbers*, vol. II, pages 615 et s. où on pourra lire la longue histoire de l'équation  $x^4 + y^4 = z^4$ . On pourra également consulter le livre de PIERRE SAMUEL, *Théorie algébrique des nombres*, Collection Méthodes, Hermann, Paris 1967, Deuxième édition revue et corrigée, Paris, 1971, page 21. On y trouve aussi, page 20, la règle de Diophante dont il sera question ci-dessous.}

Plus généralement, on a le résultat suivant, lequel est un cas très particulier du Théorème 169 de HILBERT, bien plus général. On pourra consulter *Théorie des corps de nombres algébriques*, deuxième partie, Trad. A. LEVY, *Annales de la faculté des sciences de Toulouse 3<sup>e</sup> série*, tome 2, n° 3-4, p. 455-456.

**Théorème.** *L'équation diophantienne  $x^4 + 4y^4 = z^2$  n'a pas de solutions en nombres entiers strictement positifs.*

**Démonstration.** On se servira du résultat suivant connu sous le nom de *règle* de Diophante. *Les solutions de l'équation  $x^2 + y^2 = z^2$  en  $x, y, z$ , entiers strictement positifs et premiers entre eux, sont de la forme*

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2,$$

*où  $a$  et  $b$  sont entiers, strictement positifs, premiers entre eux, l'un pair et l'autre impair.*

On utilise la méthode de la descente, en supposant que l'équation diophantienne  $x^4 + 4y^4 = z^2$  possède des solutions en nombres entiers strictement positifs. On se donne une des solutions,  $(x, y, z)$ , pour laquelle  $z$  est le plus petit possible. On observe que  $x, 2y, z$ , sont alors deux à deux premiers entre eux. En effet, si un nombre premier impair  $p$  divise deux d'entre eux, il divise le troisième et l'on aurait

$$\begin{aligned}
x &= pu, \quad y = pv, \quad z = pg, \\
p^4u^4 + 4p^4v^4 &= p^2g^2, \\
p^2(u^4 + 4v^4) &= g^2, \\
g &\text{ serait divisble par } p \text{ et l'on aurait } g = pw, \text{ d'où} \\
u^4 + 4v^4 &= w^2 \text{ où } w < z, \text{ ce qui est impossible.}
\end{aligned}$$

De même, si 2 divisait  $x$  ou  $z$ , il diviserait les deux et l'on aurait

$$\begin{aligned}
x &= 2u, \quad z = 2w, \\
16u^4 + 4y^4 &= 4w^2, \\
4u^4 + y^4 &= w^2 \text{ où } w < z, \text{ ce qui est également impossible.}
\end{aligned}$$

On écrit  $(x^2)^2 + (2y^2)^2 = z^2$ . En vertu de la règle de Diophante, on aurait

$$\begin{aligned}
x^2 &= a^2 - b^2, \quad 2y^2 = 2ab, \quad z = a^2 + b^2, \\
x^2 &= a^2 - b^2, \quad y^2 = ab, \quad z = a^2 + b^2,
\end{aligned}$$

où  $a$  et  $b$  sont des entiers non nuls, premiers entre eux, l'un pair et l'autre impair. Mais alors  $x$  est impair donc  $a^2 - b^2 = x^2 \equiv 1 \pmod{4}$ , de sorte que  $a$  est impair et  $b$  est pair !

Or,  $ab = y^2$  est un carré, donc  $a$  et  $b$  sont des carrés. De plus, on a  $x^2 + b^2 = a^2$ , donc  $a = m^2 + n^2$  et  $b = 2mn$  où  $m$  et  $n$  sont des entiers non nuls, premiers entre eux, l'un pair et l'autre impair (par la règle de Diophante). Sans nuire à la généralité, on peut supposer que c'est  $m$  qui est pair.

Puisque  $b = (2m)n$  est un carré,  $2m$  et  $n$  sont des carrés. On aurait ainsi  $2m = 4u^2$  et  $n = v^2$ . Ainsi  $4u^4 + v^4 = m^2 + n^2 = a$  où  $a$  est un carré. Or,  $a = \sqrt{z - b^2} < z^2$ , autrement dit  $\sqrt{a} < z$ , ce qui est impossible.  $\square$

De cela, on déduit aisément ceci : pour  $r$  rationnel non nul, il n'existe pas de nombre rationnel  $a$  tel que l'on ait  $(r/a)^2 = a^4 + 4$  car, en écrivant  $a = y/z$  comme fraction irréductible, on aurait  $(z^2r/a)^2 = y^4 + 4z^4$  où  $x = z^2r/a$  serait entier, ce qui est impossible.

Autrement dit, comme annoncé, la condition C2 n'est jamais satisfaite.

## BIBLIOGRAPHIE

1. Jean-Claude CARREGA, *Théorie des corps, La règle et le compas*, Nouvelle édition enrichie d'exercices, Collection Formation des enseignants, Hermann, Paris, 1989.
2. Irvin KAPLANSKY, *Fields and rings*, U. Chicago Press, (en particulier, p.50-52).
3. Peter M. NEUMANN, *Reflections on reflection in a spherical mirror*, Amer. Math. Monthly, **105** (1998) No. 6, 523-528.
4. van der WAERDEN, *Modern Algebra*, Tome 1, p.183-187, §59, [dans l'édition Frederik Ungar Publishing Co., 1949.]

JEAN-CLAUDE CARRÉGA, RÉSIDENCE HORIZON, 12 BD DE L'EUROPE, 69110  
SAINTE-FOY-LÈS-LYON, FRANCE.

*E-mail address:* `jeanclaudecarrega@orange.fr`

LABIB HADDAD, 120 RUE DE CHARONNE, 75011 PARIS, FRANCE.

*E-mail address:* `labib.haddad@wanadoo.fr`